

BURSOR & FISHER, P.A.

L. Timothy Fisher (State Bar No. 191626)
Stefan Bogdanovich (State Bar No. 324525)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
sbogdanovich@bursor.com

Attorneys for Plaintiffs

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA—EASTERN DIVISION**

ISIAH SHEPPARD, HILSCIO RIVERA,
HELENE LAUZIER-MEYER, and
BERNABE BENITEZ, individually and
on behalf of all others similarly situated,

Plaintiffs,

v.

FANTASIA TRADING LLC, and
ANKER INNOVATIONS LIMITED,
d/b/a eufy

Defendants.

Case No. 5:23-cv-02407-JGB-E

**SECOND AMENDED CLASS
ACTION COMPLAINT**

JURY TRIAL DEMANDED

1 Plaintiffs Isiah Sheppard, Hilscio Rivera, Helene Lauzier-Meyer, and Bernabe
2 Benitez (“Plaintiffs”) bring this action on behalf of themselves and all others
3 similarly situated against Defendants Fantasia Trading LLC (“Fantasia”) and Anker
4 Innovations Limited (“Anker Innovations”) doing business as eufy¹ (collectively,
5 “Defendants”), for violations of Illinois’ Biometric Information Privacy Act
6 (“BIPA”), 740 ILCS 14/1, *et seq.* The following allegations are based on their
7 counsel’s investigation and upon information and belief, except for allegations
8 concerning Plaintiffs themselves, which are based on personal knowledge.

9 **NATURE OF THE ACTION**

10 1. Plaintiffs bring this action for damages and other legal and equitable
11 remedies resulting from the illegal actions of Defendants in collecting and storing
12 their and other similarly situated individuals’ biometric identifiers without first
13 obtaining informed written consent and failing to develop, maintain, or much less
14 provide a data retention and destruction schedule, in direct violation of BIPA.

15 2. The Illinois Legislature has found that “[b]iometrics are unlike other
16 unique identifiers that are used to access finances or other sensitive information.”
17 740 ILCS 14/5(c). “For example, social security numbers, when compromised can
18 be changed. Biometric identifiers, however, are biologically unique to the
19 individual; therefore, once compromised, the individual has no recourse, is at
20 heightened risk for identify theft, and is likely to withdraw from biometric-facilitated
21 transactions.” *Id.*

22 3. In recognition of these concerns over the security of individuals’
23 biometric identifiers, the Illinois Legislature enacted BIPA, which provides, *inter*
24 *alia*, that a private entity like Defendants may not obtain and/or possess an
25

26 ¹ Although Defendants sometimes refer to their brand as “eufy” and at other times as
27 “Eufy,” defense counsel in this action has consistently referred to the brand as
28 “eufy.” For ease of reference, this Complaint shall not capitalize the first letter of the
brand name unless quoting another source.

1 individual's biometric identifiers unless it informs that person in writing that
2 biometric identifiers will be collected or stored. *See* 740 ILCS 14/15(b).

3 4. Likewise, BIPA also requires that entities collecting biometric
4 identifiers must publish and make publicly available written retention schedules and
5 guidelines for permanently destroying biometric identifiers collected. *See* 740 ILCS
6 14/15(a).

7 5. In direct violation of each of the foregoing provisions of §§ 15(b) and
8 15(a) of BIPA, Defendants collected, stored, and used—without providing notice,
9 obtaining informed written consent and without publishing a data retention
10 schedule—the biometric identifiers of Illinois delivery drivers making deliveries to
11 homes using Defendants' home security system.

12 6. In November 2022, a security researcher revealed that eufy cameras
13 uploaded images and facial recognition data to Defendants' cloud storage, which is
14 hosted by a third party (Amazon Web Services ("AWS"), a subsidiary of
15 Amazon.com, Inc.), even where the user did not sign up for cloud storage or
16 services.

17 7. Defendants eventually conceded that, even for users who did not create
18 a cloud account or agreed to the transmittal of images from their eufy camera to
19 Defendants' cloud storage, such images were nevertheless collected, transmitted, and
20 disseminated to the third-party company that hosts Defendants' cloud storage for
21 consumers, *i.e.* AWS. Defendants eventually admitted that it was sharing these
22 images with AWS in January 2023.

23 8. To be sure, BIPA independently prohibits the unconsented collection of
24 biometric identifiers that can be used to distinguish unique individuals. Nothing in
25 the text or the history of the statute gives Defendants a free pass to collect this
26 sensitive data without people's consent simply because Defendants avoid actively
27 using the biometric identifiers they collect to identify individuals, or avoid collecting
28

1 those same individuals' names, addresses, or other information to link those
2 biometric identifiers back to individuals' real-world identities.

3 9. BIPA confers on Plaintiffs, and all those similarly situated Illinois
4 residents who make home deliveries, the right to know of the risks inherently
5 presented by the collection and storage of their biometric identifiers, like the
6 geometric scans of their hands or face. Plaintiffs also have a right to know how long
7 such risks will persist while their biometric identifiers are stored and used by eufy's
8 AI.

9 10. This is particularly concerning because other home security companies
10 like Google Nest and Wyze do not allow their cameras and doorbells with facial
11 recognition capabilities to be used in Illinois.²

12 11. Plaintiffs bring this action to prevent Defendants from further violating
13 the privacy rights of Illinois delivery drivers and to recover statutory damages for
14 Defendants' unauthorized collection, storage, and use of their biometric identifiers in
15 violation of BIPA.

16 **PARTIES**

17 12. Plaintiff Isiah Sheppard is a resident of Cook County, Illinois. Plaintiff
18 Sheppard works as an Uber Eats and DoorDash delivery driver who makes deliveries
19 to customers' homes. As part of Plaintiff Sheppard's regular deliveries process, he
20 walks to the front door of the customer's residence to make the delivery. On
21 multiple deliveries, scans of Plaintiff Sheppard's face and/or hands were captured by
22 eufy's security system. Plaintiff Sheppard has a publicly available Facebook account
23 searchable by his name and which features photos of himself.

24
25
26 ² Google Store, *Nest Aware*, available at
27 https://store.google.com/us/product/nest_aware?hl=en-US&pli=1 (last accessed Oct.
28 18, 2023); Wyze, *How do I set up Friendly Faces?* (July 21, 2023), available at
[https://support.wyze.com/hc/en-us/articles/5876322908315-How-do-I-set-up-](https://support.wyze.com/hc/en-us/articles/5876322908315-How-do-I-set-up-Friendly-Faces-)
[Friendly-Faces-](https://support.wyze.com/hc/en-us/articles/5876322908315-How-do-I-set-up-Friendly-Faces-) (last accessed Oct. 18, 2023).

1 13. Plaintiff Hilscio Rivera is a resident of Cook County, Illinois. Plaintiff
2 Rivera works as an Amazon, DoorDash, Postmates, Dispatch, Veho, AxleHire and
3 Roadie delivery driver who makes deliveries to customers' homes. As part of
4 Plaintiff Rivera's regular delivery process, Plaintiff Rivera walks to the front door of
5 the customer's residence to make the delivery. On multiple deliveries, scans of
6 Plaintiff Rivera's face and/or hands were captured by eufy's security system.
7 Plaintiff Rivera has publicly available Facebook and Twitter accounts, searchable by
8 his name and which feature photos of himself.

9 14. Plaintiff Helene Lauzier-Meyer is a resident of Sangamon County,
10 Illinois. Plaintiff Lauzier-Meyer works as a DoorDash and Spark delivery driver
11 who makes deliveries to customers' homes. As part of Plaintiff Lauzier-Meyer's
12 regular deliveries process, she walks to the front door of the customer's residence to
13 make the delivery. On multiple occasions, scans of Plaintiff Lauzier-Meyer's face
14 and/or hands were captured by eufy's security system. Plaintiff Lauzier-Meyer has a
15 publicly available Facebook account searchable by her maiden name and which
16 feature images of herself.

17 15. Plaintiff Bernabe Benitez is a resident of Lake County, Illinois.
18 Plaintiff Benitez works as an UberEats delivery driver who makes deliveries to
19 customers' homes. As part of Plaintiff Benitez's regular deliveries process, he walks
20 to the front door of the customer's residence to make the delivery. On multiple
21 occasions, scans of Plaintiff Benitez's face and/or hands were captured by eufy's
22 security system. Plaintiff Benitez has publicly available Facebook and TikTok
23 accounts searchable by his last name and which feature images of himself.

24 16. Defendant Fantasia Trading LLC is a Delaware corporation with its
25 principal place of business in Ontario, California. Fantasia Trading LLC is Anker
26 Innovations Limited's wholly owned subsidiary and is under the control and
27 direction of its parent, Anker Innovations Limited. Fantasia markets and distributes
28

1 various electronic devices and accessories under the brand, Anker, as well as other
2 brands including eufy.

3 17. Defendant Anker Innovations Limited (“Anker Innovations”) is a
4 Chinese company with its principal place of business at Room 1318-19, Hollywood
5 Plaza, 610 Nathan Road, Mongkok, Kowloon, Hong Kong SAR, People’s Republic
6 of China. Anker Innovations designs, manufactures, and distributes the eufy camera
7 products for export and sale throughout the world, including throughout the United
8 States, including Illinois and California. Anker Innovations offers the eufy Security
9 App for use with eufy cameras, including by users in Illinois and California.

10 18. eufy is a home security technology brand that offers security cameras
11 supported by high quality video and artificial intelligence (“AI”) monitoring. On the
12 eufy website’s About Us page, it lists “Anker Innovations” as the company that owns
13 several brands, including eufy.³ The bottom of the page which contains hyperlinks
14 to various legal documents also lists “Fantasia Trading LLC.”⁴ eufy’s Terms of
15 Service similarly list Defendants Anker Innovations and Fantasia as “affiliated
16 companies” and purport to bind both companies into an agreement with users of the
17 “Eufy Security App and devices, eufy Baby App and devices, eufy Clean App and
18 devices, [and] EufyLife App and devices.”⁵

19 19. Defendants Anker Innovations and Fantasia (collectively,
20 “Defendants”) acted jointly to perpetrate the acts described herein, including in the
21 collection of biometric identifiers and are thus subject to joint and several liability.
22 At all times relevant to the allegations in this matter, each Defendant acted in concert
23 with, within the knowledge and approval of, and/or as the agent of the other
24

25 ³ eufy, *About Us*, <https://www.eufy.com/about?ref=footer> (last accessed May 10,
26 2024).

27 ⁴ *Id.*

28 ⁵ eufy, *Terms of Service*, <https://www.eufy.com/policies/terms-of-service?ref=footer>
(last accessed May 10, 2024).

1 Defendant within the course and scope of the agency, regarding the acts and
2 omissions alleged.

3 **JURISDICTION AND VENUE**

4 20. This Court has subject matter jurisdiction over this action pursuant to 28
5 U.S.C. § 1332(d) because there are more than 100 class members and the aggregate
6 amount in controversy exceeds \$5,000,000.00, exclusive of interest, fees, and costs,
7 and at least one class member is a citizen of a state different from Defendants.

8 21. This Court has personal jurisdiction over Defendants because Defendant
9 Fantasia Trading LLC has its principal place of business in this district, in Ontario,
10 California.

11 22. This Court has personal jurisdiction over Defendant Anker Innovations
12 because it purposefully directed its activities in this District by working with
13 Defendant Fantasia Trading, LLC to import, and thereby introduce, its eufy cameras
14 (manufactured overseas) into this District, and working with Fantasia Trading, LLC
15 in this District to thereby distribute, market, and sell the eufy camera products and
16 place them in the stream of commerce (throughout the US and Illinois, in particular)
17 from this District. *See, e.g., Yamashita v. LG Chem, Ltd.*, 62 F. 4th 496, 504 (9th
18 Cir. 2023).

19 23. Defendant Anker Innovations manufactures its products overseas and
20 imports them into this District where they are then distributed by Fantasia Trading
21 LLC in Ontario, California, in this District. In particular, Defendant Anker
22 Innovations works with Defendant Fantasia Trading, LLC to import its eufy cameras
23 into the United States through the port complex of Los Angeles and Long Beach, in
24 this District. From there, Anker Innovations works with Defendant Fantasia
25 Trading, LLC to have these eufy cameras distributed and shipped from their Ontario,
26 California distribution center(s) in this District to and throughout the US, including
27 Illinois.
28

24. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant Fantasia Trading LLC is at home in this District. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant Anker Innovations transacts business in this District, and intentionally availed itself to the laws and markets within this District.

FACTUAL ALLEGATIONS

I. eufy's Home Security System, Local AI and BionicMind AI.

25. The eufy brand is sold, marketed, and distributed by Anker Innovations throughout the United States. Defendants market, distribute, and sell their “eufy” branded camera products throughout the United States. Consumers can purchase these products online, either directly through Anker Defendants or another online retailer, or at brick-and-mortar stores like Best Buy. These camera products are specifically marketed for home security, allowing consumers to view live and recorded video of the areas around their homes and to automatically receive notifications on their cell phone, tablet, or computer regarding activity detected by the cameras, including thumbnail images when a person is detected in the cameras’ field of view.

26. The eufy brand is an emerging leader in home security systems. However, eufy “isn’t like your traditional alarm company. It’s a tech company first[.]”⁶

27. To that end, eufy sells 36 different security camera models, each equipped with on-device AI monitoring capabilities.⁷ These cameras include

⁶ Aliza Vigderman & Gabe Turner, *eufy Security System Review and Cost*, Security.org (Oct. 12, 2023) available <https://www.security.org/home-security-systems/eufy/> (last accessed May 8, 2024).

⁷ eufy, *AI Features for eufySecurity Devices*, available <https://support.eufy.com/s/article/AI-Features-for-eufySecurity-Devices> (last accessed May 8, 2024).

1 multiple models of doorbell cameras, exterior mounted and floodlight cameras, and a
2 series of base stations.⁸

3 28. eufy's AI technology is categorized as either "Local AI" or
4 "BionicMind AI." Together, they offer homeowners several different detection
5 features depending on the user's subscription and base station.

6 29. "Local AI" (eufy's on-device AI mechanism) uses an "embedded AI
7 chip" built into the cameras which provides "local, safe, and intelligent detection."⁹

8 30. The "BionicMind AI" system "has the ability to recognize familiar
9 faces, body shapes/positions, different objects, and even human behavior with its
10 machine self-learning system."¹⁰ The system conducts this analysis "locally on the
11 base station"¹¹ and is added to an already operating eufy system by incorporating the
12 proper base station. The BionicMind system enables eufy cameras to differentiate
13 between known individuals and strangers by recognizing biometric identifiers (*i.e.*,
14 details about the face's geometry as determined by facial points and contours) and
15 comparing the resulting "face templates" (or "faceprint") against the face templates
16 stored in a database.

17 31. eufy's intelligent detection arises through six unique features: (1) a
18 human detection feature where the system tries "to detect objects similar to the
19 human shape and filter out other objects like cars and animals for motion alerts;" (2)
20 facial detection where the system tries to "detect and screen faces shown in the video
21 image;" (3) human facial recognition where the system tries to "recognize faces in
22 the video image and identify the person for [the homeowner];" (4) pet detection

23 _____
24 ⁸ *Id.*

25 ⁹ *Id.*

26 ¹⁰ Jared Locke, *eufy's Latest Edge Security System Features Self-Learning AI to*
27 *Identify Family and Friends*, 9To5 Toys (Sep. 30, 2022) available
<https://9to5toys.com/2022/09/30/eufy-edge-security-system-launch/> (last accessed
28 May 8, 2024).

¹¹ *Id.*

1 where the system tries “to detect pets which appear in the video image;” (5) crying
2 detection where the system tries “to detect crying and will notify [the homeowner] if
3 necessary;” and (6) vehicle detection where the system “will catch up with the user’s
4 vehicle in the backyard or driveway.”¹²

5 32. Generally, the kind of base station the homeowner uses impacts which
6 version of eufy’s AI the homeowner can turn on. For example, the base level
7 “Original HomeBase” allows all AI-incorporated cameras and battery-operated video
8 doorbells to use the human detection and facial recognition features. The
9 “HomeBase 3”, alternatively, allows the homeowner to deploy each AI recognition
10 feature. “HomeBase E” and “HomeBase 2” allow the homeowner to use just the
11 Human Detection and Facial Recognition detection features.¹³

12 33. Although the homeowner has, in some instances, a choice of *which* base
13 station to pair with their eufy camera, “eufyCam (eufyCam [,] eufyCam E [,]
14 eufyCam 2 [,] eufyCam 2C [,] eufyCam 2 Pro [,] eufyCam 2C Pro) *must* be used
15 with HomeBase[.]”¹⁴ thereby ensuring that eufyCam and eufyCam2 cameras are AI-
16 capable. Likewise, the eufyCam 3 comes included with the HomeBase3.¹⁵

17 34. However, unlike the rest, eufy’s *wired* video doorbells allow the
18 homeowner to use the human and facial detection features without needing a base
19 station.¹⁶

20
21
22 _____
23 ¹² eufy, *supra* note 7.

24 ¹³ *Id.*

25 ¹⁴ eufy, *Does eufyCam Have to be Used with HomeBase?* available
26 [https://support.eufy.com/s/article/Does-eufy-cameras-have-to-be-used-with-](https://support.eufy.com/s/article/Does-eufy-cameras-have-to-be-used-with-HomeBase)
27 [HomeBase](https://support.eufy.com/s/article/Does-eufy-cameras-have-to-be-used-with-HomeBase) (last accessed May 8, 2024) (emphasis added).

28 ¹⁵ Cool Blue, *What are the Differences Between the EufyCam 3, 2 Pro, and 2?*
available [https://www.coolblue.nl/en/advice/compare-the-eufycam-3-with-the-2-pro-](https://www.coolblue.nl/en/advice/compare-the-eufycam-3-with-the-2-pro-and-2.html)
and-2.html (last accessed May 8, 2024).

¹⁶ eufy, *supra* note 7.



35. Regardless of which camera is used, eufy's Local AI system is remarkably accurate. As eufy boasts, its on-camera AI human detection feature "accurately detect[s] humans and vehicles" 95% of the time.¹⁷ Likewise, users can enhance their system's AI capabilities by adding eufy's BionicMind AI-equipped base stations to their security systems.¹⁸ eufy's BionicMind AI system, which can be added simply by connecting a new base station,¹⁹ "uses self-learning algorithms after every facial and body shape scan to improve recognition accuracy to more than 99.9% over time—no matter what [the subject is] wearing and how [the subject] approach[es] the camera."²⁰

¹⁷ eufy, *SoloCam S340*, available https://www.eufy.com/solocam-s340?utm_source=google&utm_medium=search&utm_content=always&utm_campaign=us_security_edge_conversion_search_eufycam_purchase_ost_M3_bb&utm_term=19626718763_144313519606_676641948951&gclid=CjwKCAjwvrOpBhBdEiWAR58-3NdpFPiGlnThHvpGuSIhMB31i0N0GkYya92NvW0IIXAjSnobXtGefBoCVVoQAvD_BwE (last accessed May 8, 2024).

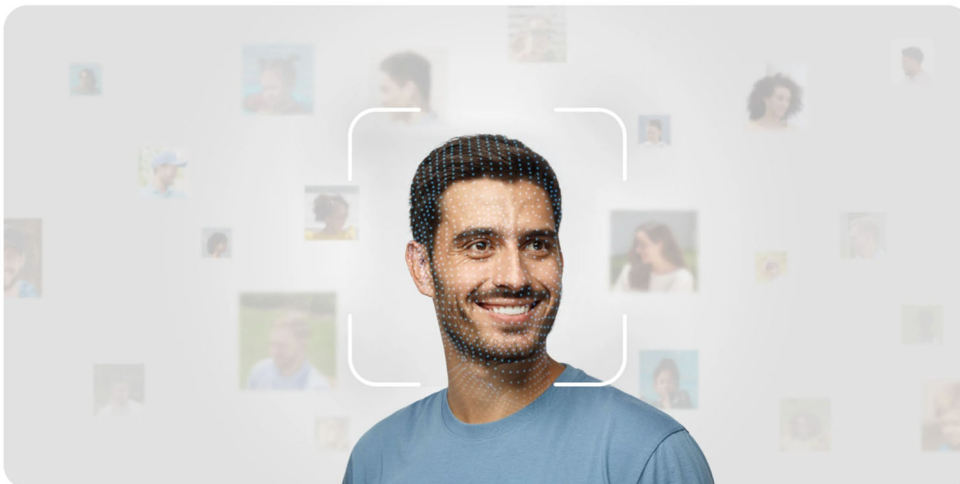
¹⁸ See Jennifer Pattison Tuohy, *eufy's Impressive New Smart Cameras Use AI to Identify You and Your Pets*, The Verge (Sep. 30, 2022) available <https://www.theverge.com/2022/9/29/23378472/eufy-homebase-3-eufycam-3-price-release-date-specs> (last accessed May 8, 2024).

¹⁹ See eufy, *supra* note 17. ("HomeBase 3 has expandable local storage up to 16 TB, while adding the power of BionicMind for an accurate AI experience.")

²⁰ eufy, *eufyCam 3*, available <https://us.eufy.com/pages/security-eufycam3> (last accessed May 8, 2024).

Self-Learning Facial Recognition

BionicMind™ uses self-learning algorithms after every facial and body shape scan to improve recognition accuracy to more than 99.9% over time—no matter what you're wearing or how you approach the camera.



36. Human detection, available for “Local AI” and “BionicMind AI” users, “detects and captures motion . . . for accurate object classification.”²¹

eufyCam 3 | eufyCam 3C

Overview Compare

Buy Now

BionicMind™ Identifies Your Family

Security is beyond detection and embracing recognition with BionicMind™. Now, you can know instantly when there's a stranger at the door, and when your family arrives home safe.



37. The technology “works in two steps[.]”²² First, “[w]hen the camera detects motion in its field of view, the AI engine analyzes the figure to determine if it

²¹ eufy, *How Does the Human Detection Technology Work?* available <https://support.eufy.com/s/article/How-does-the-Human-Detection-technology-work> (last accessed May 8, 2024).

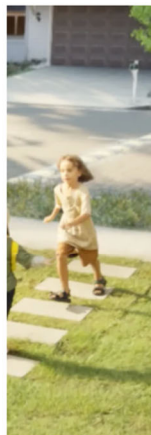
²² *Id.*

is a human being or not.”²³ Second, “if the captured face meets the AI engine’s analysis parameters, the AI engine will try to capture the face and then send a notification to the user.”²⁴ This step allows the system to use the captured biometric identifiers in two scenarios.

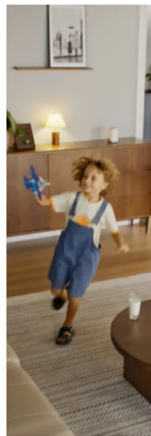
38. One such feature is “cross camera tracking” where, once stored with the proper base station connected, eufy’s system will “automatically compile shots of **the same event and person** and organize them chronologically into a single clip”²⁵ if an event occurs within the view of multiple cameras.

Cross Camera* Tracking

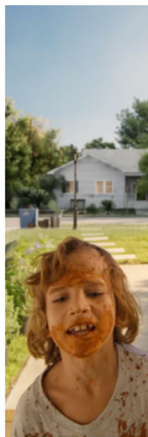
Automatically splice together videos of the same event or person, in order of occurrence, across cameras*. Creates a coherent event video allowing you to quickly and comprehensively understand events completely.



Captured on SoloCam S340



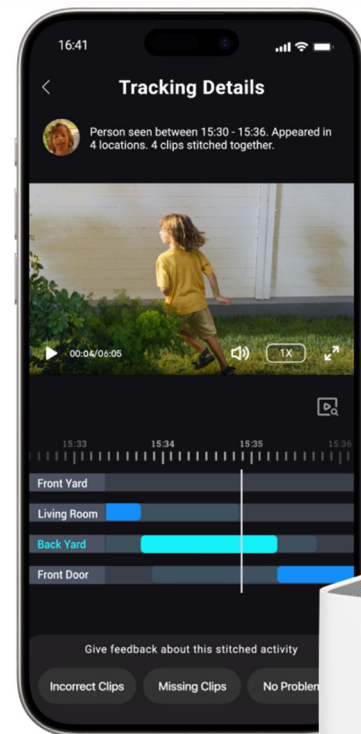
Captured on Indoor Cam S350



Captured on Video Doorbell E340



Captured on Floodlight Cam E340



39. As eufy explains, “[w]hen the same individual appears across multiple cameras within a specified timeframe, the system automatically locates and merges

²³ *Id.*

²⁴ *Id.*

²⁵ Anthony Spadafora, *Eufy’s New Security Cameras Use AI for Cross-Camera Tracking—Here’s How it Works*, Yahoo! Tech (Sep. 26, 2023) available <https://finance.yahoo.com/news/eufy-security-cameras-ai-cross-230048637.html>. (last accessed May 8, 2024) (emphasis added).

1 these footage [sic] into a single video” so that the homeowner can “easily review the
2 entire activity **of that specific individual** in a single video.”²⁶

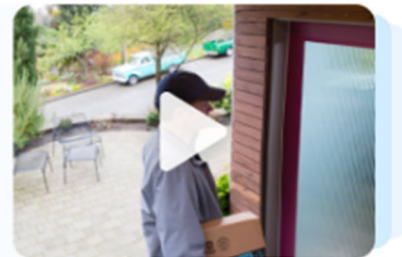
3 40. To piece the footage together, the BionicMind base station “analyzes
4 the video content and stitches it together in-real [sic]” time and, “[a]fter each camera
5 has finished recording and saving videos to [the base station], [] re-analyzes the
6 video content for splicing.”²⁷ Cameras that are not compatible with BionicMind base
7 stations cannot stitch images together in real time and, instead, analyze saved video
8 after recording has ended.²⁸

9 41. The homeowner then receives a notification alerting them that the
10 device has either detected an already cataloged face like a friend or a new, unknown
11 visitor like a delivery driver:

12 07:10 AM, seen a person activity.



16 Appeared in 2 locations.
17 12 clips stitched together.



18
19
20
21
22
23 ²⁶ eufy Support, *Introducing the Cross-Camera Tracking Function in the eufy*
24 *Security App*, eufy available [https://support.eufy.com/s/article/Introducing-the-](https://support.eufy.com/s/article/Introducing-the-Cross-Camera-Tracking-Function-in-the-eufy-Security-App)
25 *Cross-Camera-Tracking-Function-in-the-eufy-Security-App* (last accessed May 8,
26 2024) (emphasis added).

27 ²⁷ *Id.*

28 ²⁸ *See Id.* (“Cameras that are compatible with HomeBase 3 storage, but not with
HomeBase 3 BionicMind [] A.I., will only be able to use the Look-Back Tracking
Function. . .”).

When multiple individuals appear at the same time, a separate event will be created for each individual.

08:30 AM, seen their appearing together.



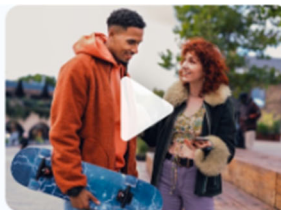
Robert

Appeared in 2 locations.
12 clips stitched together.



Lia

Appeared in 2 locations.
12 clips stitched together.



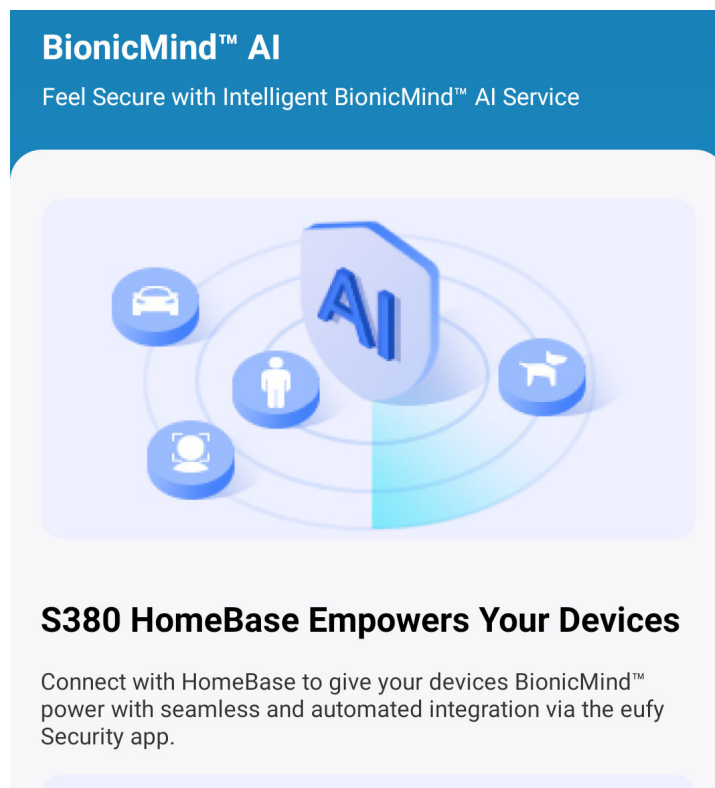
42. eufy is capable of making these identifications by storing and analyzing biometric-identifier data so the AI can “keep learning the details of the characteristics of people, including different angles of the face and bodies” to “help the AI recognize a person more accurately and quickly.”²⁹ That data is then accessible to the user via the eufy Security App.³⁰

43. eufy, through its marketing, actively invites users to take advantage of its BionicMind AI feature, thereby enabling collection and capture of biometric identifiers, as shown by a screenshot posted to a eufy community forum page by a eufy camera user.³¹

²⁹ eufy Support, *What is the self-learning AI in the HomeBase 3?* eufy (Dec. 1, 2022) available <https://support.myeufy.com.au/support/solutions/articles/73000597074-what-is-the-self-learning-ai-in-homebase-3-> (last accessed May 8, 2024).

³⁰ *Id.*

³¹ eufy, *Please Empower All Paired Cameras with BionicMind*, available <https://community.security.eufy.com/t/please-empower-all-paired-cameras-with-bionicmind/3724469/2> (last accessed May 2, 2024).



44. In marketing the service, eufy encourages its users to “[c]onnect with HomeBase to give your devices BionicMind power with seamless and automated integration via the eufy Security app.”

II. The eufy Security App and Defendants’ Data Storage Practices

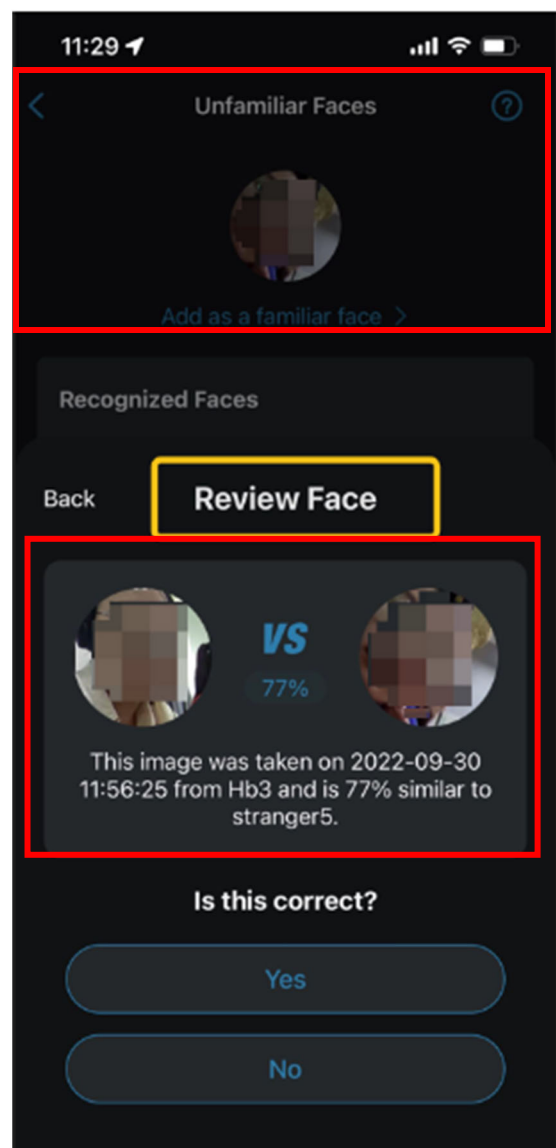
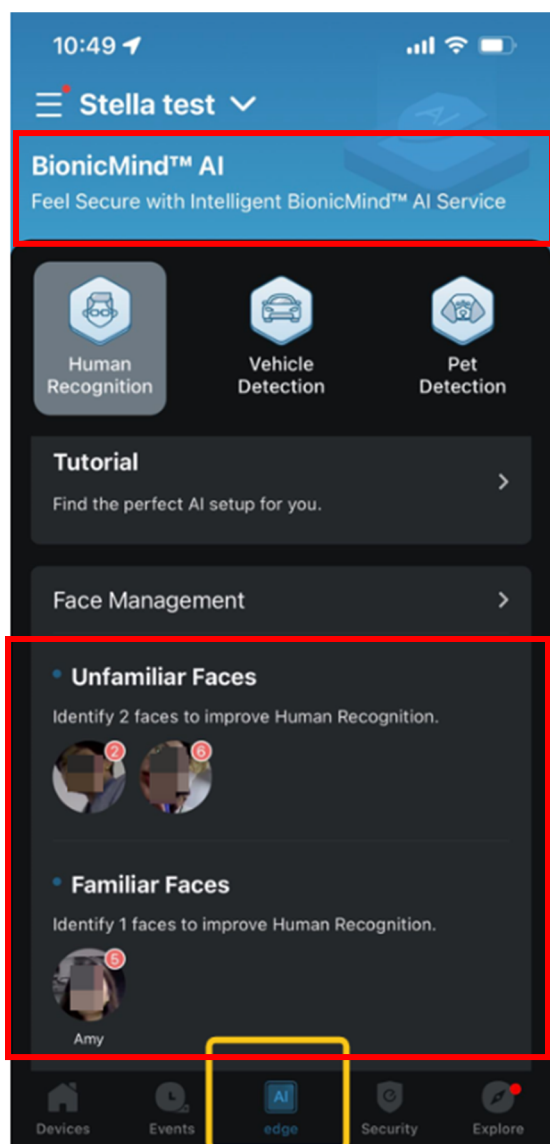
45. The cameras’ labels advertise and warrant that “[a]ll your footage is securely stored locally[,] [e]nsuring the videos you record are for you and only you.” However, this was not the case.

46. Consumers who purchase a eufy camera must use the eufy Security App smartphone application. The eufy Security App allows users to access their cameras, view live and historical video feeds, and adjust the cameras’ settings. The cameras communicate with the eufy Security App to provide users notifications, such as when the camera detects activity.³² As referenced above, the eufy cameras communicate

³² Google Play, *eufy Security*, available https://play.google.com/store/apps/details?id=com.oceanwing.battery.cam&hl=en_US&gl=US (last accessed Apr. 30, 2024).

1 with the eufy Security App to provide user notifications, such as notification of
2 activity on the cameras.

3 47. The eufy App also allows users to access and review specific data points
4 such as scanned faces (*i.e.*, biometric identifiers):



24 48. Ensuring that its products have access to biometric identifiers is critical
25 to some of eufy's marketed features. In fact, eufy readily admits that "[t]he Cross-
26 Camera Tracking function depends on a human feature recognition algorithm [sic]
27 that determines the similarity of an individual's appearance in two videos to stitch
28

1 them together. Even if the face is not visible in the video, videos of similar-looking
2 individuals are still identified and stitched together.”³³

3 49. And, although eufy represents that its AI and biometric collections are
4 stored locally, as recently as December 2022 (well within BIPA’s five-year statute of
5 limitations from the commencement of this action), “it was revealed that Anker’s
6 eufy was sending data from its cameras to the cloud, despite”³⁴ advertising “several
7 of its security cameras with the promise that video footage and other data are local
8 only.”³⁵ eufy marketed that “its cameras and video doorbells [used] local-only
9 recording for enhanced security, but a security researcher found that the company
10 was uploading images from the cameras to AWS servers alongside facial recognition
11 data.”³⁶ Specifically, the researcher, in testing one of eufy’s devices, found that “[t]he
12 doorbell’s camera was uploading facial recognition data from the camera to Eufy’s
13 cloud servers with identifiable information attached, and that this data wasn’t
14 actually removed from Eufy’s servers when the related footage had been deleted
15 from the Eufy app.”³⁷ The researcher, in making this discovery, also expressed
16 concern that “Eufy could link footage collected from different cameras and apps to
17 individuals using facial recognition.”³⁸

18
19
20 ³³ eufy, *supra* note 26.

21 ³⁴ Ben Schoon, *Eufy Will Add a Disclosure to its App Following Security Concerns*
22 *but Still Denies Glaring Security Holes*, 9to5Google (Dec. 5, 2022) available
<https://9to5google.com/2022/12/05/eufy-disclosure-cloud/> (last accessed May 8,
2024).

23 ³⁵ Ben Schoon, *Eufy Caught Lying About Local-Only Security Cameras with Footage*
24 *Sent to Cloud, Accessible in Unencrypted Streams*, 9to5Google (Dec. 1, 2022)
available <https://9to5google.com/2022/12/01/eufy-camera-cloud-security-leak/> (last
accessed May 8, 2024).

25 ³⁶ Ben Schoon, *supra* note 34.

26 ³⁷ Ben Schoon, *supra* note 35.

27 ³⁸ Joel R. McConvey, *Eufy Doorbell Cameras Uploading Facial Recognition Data to*
28 *the Cloud Without Consent*, Biometric Update (Nov. 30, 2022) available
[https://www.biometricupdate.com/202211/eufy-doorbell-cameras-uploading-facial-](https://www.biometricupdate.com/202211/eufy-doorbell-cameras-uploading-facial-recognition-data-to-the-cloud-without-consent)
[recognition-data-to-the-cloud-without-consent](https://www.biometricupdate.com/202211/eufy-doorbell-cameras-uploading-facial-recognition-data-to-the-cloud-without-consent) (last accessed May 8, 2024).

1 50. AWS Servers are servers offered by Amazon.com to companies like
2 Defendants as “low-cost ways to deliver their websites and web applications” to
3 users.³⁹

4 51. That researcher’s findings were supported by security firm SEC Consult
5 who summarized two years of analyzing a eufyCam, noting a similar transfer of
6 thumbnails through a cloud service. The company also saw the weak keys,
7 suggesting “hard-coded encryption/decryption keys which are *identical for all sold*
8 *Homebase devices*,” though it was unclear for what the keys were being used.⁴⁰

9 52. The data wrongfully collected, transmitted, and disseminated by
10 Defendants includes biometric identifiers. One of the most prevalent uses of
11 biometric identifiers is in facial recognition technology, which works by scanning a
12 human face or an image thereof, extracting facial feature data based on specific
13 identifiers, and comparing the resulting “face template” (or “faceprint”) against
14 templates stored in a database.

15 53. In fact, once this and other reckless data management practices were
16 discovered, eufy acknowledged in a January 2023 press release that “[p]reviously,
17 we [had] one device, the Video Doorbell Dual, that sent and stored an image of the
18 user to our secure cloud ... First, the purpose of sending a user image from the eufy
19 App to our devices is to give the local facial recognition software a baseline to run its

20
21
22
23 ³⁹ See Amazon Web Service, *AWS*, available
24 https://aws.amazon.com/free/webapps/?gclid=Cj0KCQiA2eKtBhDcARIsAEGTG42H9ebgefFKYVCD5h-YNFJ39VpoUAvyk1r0DUwhVMIM-iwBVJph6noaAsOaEALw_wcB&trk=0859629e-29af-428f-ab68-152ecf240a0b&sc_channel=ps&ef_id=Cj0KCQiA2eKtBhDcARIsAEGTG42H9ebgefFKYVCD5h-YNFJ39VpoUAvyk1r0DUwhVMIM-iwBVJph6noaAsOaEALw_wcB:G:s&s_kwcid=AL!4422!3!531871356653!p!!g!!aws%20web%20hosting!11086666988!11T455470529 (last accessed May 8, 2024).

25
26
27 ⁴⁰ SEC Consult, *The eufyCam Long-Term Observation*, SEC CONSULT (Nov. 24,
28 2022), available <https://sec-consult.com/blog/detail/the-eufycam-long-term-observation/> (last accessed May 3, 2024) (emphasis added).

1 algorithm.”⁴¹ However, as would be revealed, Defendants’ storing facial thumbnails
2 in its cloud was actually occurring across all eufy devices and such external storage
3 was necessary to allow eufy Security App users to receive push notifications with
4 faces. “[T]hese thumbnails [were] temporarily sent to Eufy’s AWS servers before
5 arriving in [a eufy Security App] notification.”⁴²

6 54. After this revelation, Defendants stated that they were “revising the
7 push notifications option language in the eufy Security app to clearly detail that push
8 notifications with thumbnails require preview images that will be temporarily stored
9 in the cloud.”^{43, 44}



20 ⁴¹ Sean Hollister, *Anker Finally Comes Clean About Its Eufy Security Cameras*, The
21 Verge (Jan. 31, 2023) available <https://www.theverge.com/23573362/anker-eufy-security-camera-answers-encryption> (May 8, 2024) (Emphasis added).

22 ⁴² Christopher Boyd, *eufy “No Cloud” Security Cameras Streaming Data to the*
23 *Cloud*, MALWAREBYTES LABS (Dec. 5, 2022) available
24 <https://www.malwarebytes.com/blog/news/2022/12/is-your-home-security-system-storing-data-100-locally#:~:text=%E2%80%9CWe%20are%20revising%20the%20push,consumer%20Dfacing%20marketing%20materials.%E2%80%9D> (last accessed Apr. 30, 2024).

25 ⁴³ *Id.*

26 ⁴⁴ Amazon.com, *eufy Security Indoor Cam E220, Pan & Tilt, Indoor Security*
27 *Camera, 2K -3 MP Wi-Fi Plug-In, Voice Assistant Compatibility, Night Vision,*
28 *Motion Tracking, HomeBase 3 Compatible, Motion Only Alert*, available
<https://www.amazon.com/eufy-Security-Assistant-Compatibility-Tracking/dp/B0856W45VL> (last accessed May 8, 2024).

1 55. Defendants were aware of the transmissions. Defendants specifically
2 designed and manufactured the cameras to communicate data, over the internet, often
3 to Defendants' own servers and with its security app. Despite Defendants' exclusive
4 knowledge regarding the design and operation of the cameras, the AI, its App, and
5 cloud servers, Defendants continued to market the cameras as only storing data
6 locally. It wasn't until third-party security experts examined the cameras and
7 published their results that Defendants were forced to address these transmissions.

8 56. Indeed, the Illinois Legislature was motivated to enact BIPA to protect
9 unauthorized disclosure of biometric identifiers because "[b]iometrics are unlike
10 other unique identifiers that are used to access finances or other sensitive
11 information." 740 ILCS 14/5(c). Accordingly, because "[b]iometrics [] are
12 biologically unique to the individual [,] once compromised, the individual has no
13 recourse, is at heightened risk for identify theft, and is likely to withdraw from
14 biometric-facilitated transactions." *Id.*

15 57. Due to these concerns, BIPA provides, *inter alia*, that private entities
16 like Defendants may not obtain and/or possess an individual's biometric identifiers
17 unless it informs that person in writing that biometric identifiers will be collected or
18 stored. *See* 740 ILCS 14/15(b).

19 58. Likewise, BIPA also requires that entities collecting biometric
20 identifiers publish and make publicly available written retention schedules and
21 guidelines for permanently destroying biometric identifiers collected. *See* 740 ILCS
22 14/15(c).

23 **III. Illinois' Biometric Information Privacy Act**

24 59. BIPA defines biometric identifiers as "a retina or iris scan, fingerprint,
25 voiceprint, or scan of hand or face geometry." 740 ILCS 14/10 (emphasis added).

26 60. Facial geometry is a permanent, unique biometric identifier associated
27 only with a specific person. Collecting and storing a person's face geometry exposes
28 them to serious and irreversible privacy risks. For example, if a device or database

1 containing stored images of facial geometry is hacked, breached, or otherwise
2 compromised, the person has no means by which they can prevent identity theft or
3 unauthorized hacking of secure devices which use facial recognition to grant access.

4 61. Recognizing the need to protect citizens from these risks, Illinois
5 enacted the Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (“BIPA”) in
6 2008, to regulate companies that collect and store biometric identifiers, such as facial
7 geometry. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276.

8 62. Accordingly, BIPA makes it unlawful for a company to, *inter alia*,
9 “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a
10 customer’s biometric identifiers ... unless it first:

- 11 1) informs the subject ... in writing that a biometric identifier ... is being
12 collected or stored;
- 13 2) informs the subject ... in writing of the specific purpose and length of
14 term for which a biometric identifier ... is being collected, stored, and
15 used; and
- 16 3) receives a written release executed by the subject of the biometric
17 identifier ... or the subject’s legally authorized representative.”

18 740 ILCS 14/15(b).

19 63. Additionally, Section 15(a) of BIPA requires that entities in possession
20 of biometric identifiers publish a schedule detailing its retention and destruction
21 plans concerning the biometric identifiers in its possession.

22 64. Section 15(a) of BIPA provides that:

23 A private entity in possession of biometric identifiers ... must develop a
24 written policy, made available to the public, establishing a retention schedule
25 and guidelines for permanently destroying biometric identifiers ... when the
26 initial purpose for collecting or obtaining such identifiers or information has
27 been satisfied or within 3 years of the individual’s last interaction with the
28 private entity, whichever occurs first.

740 ILCS 14/15(a).

1 65. As alleged below, Defendants' practices of collecting, storing, and
2 using delivery drivers' biometric identifiers without informed written consent
3 violated all three prongs of § 15(b) of BIPA. Furthermore, Defendants violate §
4 15(a) of BIPA by failing to publish and make publicly available any written policy
5 regarding Defendants' schedule and guidelines for retaining and permanently
6 destroying individuals' biometric identifiers.

7 **IV. Defendants Violate Illinois' Biometric Information Privacy Act**

8 66. Unbeknownst to Plaintiffs, and in direct violation of § 15(b)(1) of
9 BIPA, Defendants collected, scanned, and then indefinitely stored in an electronic
10 database, Plaintiffs' biometric identifiers when Plaintiffs and Class Members made
11 deliveries to the homes of Defendants' customers who used Defendants' security
12 system. Each time Plaintiffs and Class Members made a delivery to Defendants'
13 customers' homes, Defendants' cameras collected Plaintiffs' face and/or hand
14 geometry and stored the images of Plaintiffs' face and body geometry in an
15 electronic database without ever informing Plaintiffs in writing that it was doing so.

16 67. Moreover, in direct violation of §§ 15(b)(2) and 15(b)(3) of BIPA,
17 Defendants never informed Plaintiffs and Class Members who had their biometric
18 identifiers collected, of the specific purpose and length of time for which their
19 biometric identifiers would be collected, stored, and used, nor did Defendants ever
20 obtain a written release.

21 68. Finally, and in direct violation of § 15(a) of BIPA, Defendants failed to
22 publish policies for public access identifying its retention schedules or guidelines for
23 permanently destroying any of these biometric identifiers.

24 **CLASS ALLEGATIONS**

25 69. Plaintiffs bring this matter on behalf of themselves and all similarly
26 situated in the following class:

27 **Illinois Class:** All natural persons in Illinois who are delivery drivers
28 and who, when making deliveries, had their biometric identifiers

1 collected, stored, and scanned by eufy cameras and software from
2 November 27, 2018, to present.

3 70. Excluded from the Class are: (1) any Judge or Magistrate presiding over
4 this action and any members of their families; (2) Defendants, Defendants'
5 subsidiaries, parents, successors, predecessors, and any entity in which Defendants
6 or its parents have a controlling interest and their current or former employees,
7 officers, and directors; and (3) Plaintiffs' counsel and Defendants' counsel.

8 71. The members of the Class are so numerous that joinder of all members
9 is impracticable. While the exact number of Class members is unknown to Plaintiffs
10 at this time, such information can be ascertained through appropriate discovery from
11 records maintained by Defendants and its agents.

12 72. Plaintiffs reserve the right to expand, limit, modify, or amend the class
13 definition, including the addition of one or more Subclasses, in connection with their
14 motion for class certification, or at any other time, based on, *inter alia*, changing
15 circumstances and new facts obtained.

16 73. **Numerosity:** Class Members are so numerous that joinder of all
17 members is impracticable. Plaintiffs believe that there are thousands of delivery
18 drivers who are Class Members described above who have been damaged by
19 Defendants' unlawful collecting, storing, and using of their biometric identifiers.

20 74. **Commonality and Predominance:** The questions of law and fact
21 common to the class which predominate over any questions which may affect
22 individual class members include, but are not limited to:

- 23 a. whether Defendants collected or otherwise obtained Plaintiffs' and the
Class's biometric identifiers;
- 24 b. whether Defendants properly informed Plaintiffs and the Class that it
25 collected, used, and stored their biometric identifiers;
- 26 c. whether Defendants obtained a written release (as defined by 740 ILCS
27 14/10) to collect, use, and store Plaintiffs' and the Class's biometric
28 identifiers;

- d. whether Defendants developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers when the initial purpose for collecting or obtaining such identifiers has been satisfied or within 3 years of their last interaction, whichever comes first;
- e. whether Defendants destroyed Plaintiffs' and the Class's biometric identifiers once that information was no longer needed for the purpose for which it was originally collected; and
- f. whether Defendants' violations of BIPA were committed intentionally, recklessly, or negligently.

75. **Typicality:** The claims of the named Plaintiffs are typical of the claims of the Class because the named Plaintiffs, like other members of the Class, made deliveries to customer's homes and had their biometric identifiers collected, stored, and analyzed by Defendants' cameras and software without providing consent, nor did Defendants provide Plaintiffs and Class Members with written policy made publicly available establishing a schedule and procedure for permanently destroying Plaintiffs' and Class Members' biometric identifiers.

76. **Adequate Representation:** Plaintiffs have retained and are represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation. Plaintiffs and their counsel are committed to vigorously prosecuting this class action. Neither Plaintiffs, nor their counsel, have any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiffs are able to fairly and adequately represent the interests of the Class. Plaintiffs have raised viable statutory claims of the type reasonably expected to be raised by members of the Class and will vigorously pursue those claims. If necessary, Plaintiffs may seek leave of this Court to amend this complaint to include additional Class Representatives to represent the Class or additional claims as may be appropriate.

77. **Superiority:** A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of

1 the claims of all members of the Class is impracticable. Even if every member of the
2 Class could afford to pursue individual litigation, the Court system could not. It
3 would be unduly burdensome to the courts in which individual litigation of
4 numerous cases would proceed. Individualized litigation would also present the
5 potential for varying, inconsistent, or contradictory judgments, and would magnify
6 the delay and expense to all parties and to the court system resulting in multiple trials
7 of the same factual issues. By contrast, the maintenance of this action as a class
8 action, with respect to some or all of the issues presented herein, presents fewer
9 management difficulties, conserves the resources of the parties and of the court
10 system and protects the rights of each member of the Class. Plaintiffs anticipate no
11 difficulty in the management of this action as a class action. Class-wide relief is
12 essential to compel compliance with BIPA.

13 **COUNT I**

14 **Violation of 740 ILCS 14/15(b)**
15 **(On Behalf of Plaintiffs and the Class)**

16 78. Plaintiffs incorporate the foregoing allegations as if fully set forth
17 herein.

18 79. BIPA makes it unlawful for any private entity to, among other things,
19 “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a
20 customer’s biometric identifiers ... unless it first: (1) informs the subject . . . in
21 writing that a biometric identifier ... is being collected or stored; (2) informs the
22 subject . . . in writing of the specific purpose and length of term for which a
23 biometric identifier ... is being collected, stored, and used; and (3) receives a written
24 release executed by the subject of the biometric identifier or information. . .” 740
25 ILCS 14/15(b).

26 80. Defendants failed to comply with these BIPA mandates.

27 81. Fantasia Trading LLC is a limited liability company doing business as
28 eufy and thus qualifies as a “private entity” under BIPA. *See* 740 ILCS 14/10.

1 82. Anker Innovations Limited is a company doing business as eufy and
2 thus qualifies as a “private entity” under BIPA. *See Id.*

3 83. Plaintiffs and Class Members are delivery drivers in Illinois who had
4 their “biometric identifiers,” including scans of face and hand geometry, collected,
5 captured, received, or otherwise obtained by Defendants from video and/or images
6 recorded by a eufy device and scanned by eufy software to differentiate between
7 humans and non-human entrants on the camera-owner’s property.

8 84. Plaintiffs and Class Members’ face, body, and hand geometry was
9 stored and mechanically measured to create numerical representations used as “face
10 templates” that can be used to uniquely identify Plaintiffs and Class Members. *See*
11 740 ILCS 14/10.

12 85. Defendants collected, captured, or otherwise obtained Plaintiffs’ and
13 Class Members’ “biometric identifiers” (which it used to create and store uniquely
14 identifying face geometry) without first obtaining signed written releases, as required
15 by 740 ILCS 14/15(b)(3), from any of Plaintiffs.

16 86. Plaintiffs’ and Class members’ scans of face and/or hand geometry
17 constitute “biometric identifiers.” *See* 740 ILCS 14/10.

18 87. Defendants never informed Plaintiffs or members of the Class in writing
19 that their biometric identifiers were being collected, captured, stored, and/or used,
20 nor did Defendants inform Plaintiffs and members of the Class in writing of the
21 length of time for which their biometric identifiers were being collected, stored, and
22 used as required by 740 ILCS 14/15(b)(1)-(2).

23 88. By collecting, capturing, storing, and/or using Plaintiffs’ and members
24 of the Class’s biometric identifiers as described herein, Defendants violated
25 Plaintiffs’ and the Class’s right to privacy in their biometric identifiers as set forth in
26 BIPA. *See* 740 ILCS 14/1, *et seq.*

27 89. And while Plaintiffs and members of the Class are not required to plead
28 that Defendants can link these identifiers back to Plaintiff and Class Members,

1 Defendants are nonetheless able to do so. This is because most people have
2 Facebook, Twitter, Snapchat, or other social media accounts bearing their real-life
3 names and photos. Those real-life names and photos are publicly available to allow
4 other unconnected people to find them. Defendants are capable of employing the
5 very same facial recognition technology used in its cameras and base stations on
6 someone's public facing social media profile to match that individual's biometric
7 identifiers collected from their public online photos to their biometric identifiers
8 collected by its cameras and base station during a home visit. As such, Defendants'
9 human recognition feature is capable identifying an individual.

10 90. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory
11 relief; (2) injunctive and equitable relief as is necessary to protect the interest of
12 Plaintiffs and the Class by requiring eufy comply with BIPA's requirements for the
13 collection, storage, and use of "biometric identifiers" as described herein; (3)
14 statutory damages of \$1,000.00 pursuant to 740 ILCS 14/20 for each negligent
15 violation of BIPA committed by eufy; (4) statutory damages of \$5,000.00 pursuant
16 to 740 ILCS 14/20 for each intentional or reckless violation of BIPA committed by
17 eufy; and (5) reasonable attorneys' fees and costs and other litigation expenses
18 pursuant to 740 ILCS 14/20(3).

19 **COUNT II**
20 **Violation of 740 ILCS 14/15(a)**
21 **(On Behalf of Plaintiffs and the Class)**

22 91. Plaintiffs incorporate the foregoing allegations as if fully set forth
23 herein.

24 92. BIPA mandates that companies in possession of biometric data establish
25 and maintain a satisfactory biometric data retention and deletion policy.
26 Specifically, those companies must: (i) make publicly available a written policy
27 establishing a retention schedule and guidelines for permanent deletion of biometric
28 data (at most three years after the company's last interaction with the individual);

1 and (ii) actually adhere to that retention schedule and actually delete the biometric
2 identifiers. *See* 740 ILCS 14/15(a).

3 93. Defendants failed to comply with these BIPA mandates.

4 94. Plaintiffs are individuals who had their “biometric identifiers” captured
5 and/or collected by Defendants, as explained in detail above. *See* 740 ILCS 14/10.

6 95. Plaintiffs’ biometric identifiers consisted of scans of face geometry, as
7 defined by BIPA. *See* 740 ILCS 14/10.

8 96. Defendants failed to provide a publicly available retention schedule or
9 guidelines for permanently destroying Plaintiffs’ biometric identifiers as specified by
10 BIPA. *See* 740 ILCS 14/15(a).

11 97. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory
12 relief; (2) injunctive and equitable relief as is necessary to protect the interests of
13 Plaintiffs and the Class by requiring Defendants to comply with BIPA’s
14 requirements for the collecting, storing, and using biometric identifiers as described
15 herein; (3) statutory damages of \$5,000 for each intentional and/or reckless violation
16 of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of
17 \$1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4)
18 reasonable attorneys’ fees and costs and other litigation expenses pursuant to 740
19 ILCS 14/20(3).

20 **PRAYER FOR RELIEF**

21 WHEREFORE, Plaintiffs, individually and on behalf of all others similarly
22 situated, seek judgement against Defendants as follows:

- 23 A. Certifying this case as a class action on behalf of the Class defined
24 above, appointing Plaintiffs as representatives of the Class, and
appointing their counsel as Class Counsel of the Class;
- 25 B. Declaring that Defendants’ actions, as set out above, violate BIPA, 740
26 ILCS 14/1, *et seq.*, with respect to Plaintiffs and Class Members;
- 27 C. Awarding statutory damages to Plaintiffs and Class Members of
28 \$1,000.00 pursuant to 740 ILCS 14/20(1) for each violation of BIPA

1 committed negligently, and \$5,000.00 pursuant to 740 ILCS 14/20(2)
2 for each violation of BIPA committed intentionally or recklessly;

- 3 D. Awarding injunctive and other equitable relief as is necessary to protect
4 the interests of Plaintiffs and members of the Class, including *inter alia*,
5 an order requiring Defendants to collect, store, and use biometric
6 identifiers in compliance with BIPA;
7 E. Awarding Plaintiffs and the Class their reasonable litigation expenses
8 and attorneys' fees pursuant to BIPA;
9 F. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the
10 extent allowable;
11 G. Awarding Plaintiffs and the Class such other and further relief as equity
12 and justice may require.

JURY TRIAL DEMANDED

11 Under Federal Rule of Civil Procedure 38, Plaintiffs, individually and on behalf
12 of the members of the Class, exercise their right under the Seventh Amendment to the
13 United States Constitution and demand a trial by jury.
14

15 Dated: May 13, 2024

Respectfully submitted,

BURSOR & FISHER, P.A.

18 By: /s/ L. Timothy Fisher
19 L. Timothy Fisher

20 L. Timothy Fisher (State Bar No. 191626)
21 Stefan Bogdanovich (State Bar No. 324525)
22 1990 North California Blvd., Suite 940
23 Walnut Creek, CA 94596
24 Telephone: (925) 300-4455
25 Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
sbogdanovich@bursor.com

Attorneys for Plaintiffs